Security attacks in S-WBANs on IoT based Healthcare Applications

Jacob John, Mariam Sunil Varkey, Selvi M

***Abstract:** The internet exists as a global interconnection network for information sharing, commerce, and entertainment. The usage of internet has grown tremendously over the past decade in the field of E- health care monitoring system. In E- health care monitoring systems, Smart Wireless Body Area Networks (S-WBANs) is one among such technologies and is being explored. S-WBANs are primarily used as a smart object with computer-assisted rehabilitation. They serve as a remote monitoring service in smart electronic healthcare to continuously measure the vital parameters like heart rate, insulin level, body temperature, etc. They are thereby providing doctors with early detection of a patient's medical conditions. However, sharing of sensitive personal data over a wireless network requires a high level of security. Since any breach in the system security will lead to a direct violation of the patient's privacy. In order to address the security vulnerability of the existing system, in this paper a block chain based Smart Wireless Body Area Networks has been proposed to provide better security with enhanced privacy and access control for E- health care monitoring system. Moreover, the proposed system enhances the scalability and provides mitigation against all the security attacks in IoT Environment.*

***Keywords**: Block Chain, IoT, E-Health monitoring system, security threats, Smart Wireless Body Area Networks.*

I. INTRODUCTION

By the year 2020, 44% of the total world's population will have access to the Internet. Furthermore, China and India would be the "world's online superpowers" and would comprise one-third of the total Internet users[1]. This is evident with the extensive amount of e-commerce opportunities available in India and China, such as Alibaba, Flipkart, and Amazon, that would help stimulate the online presence of a user. According to a World Health Organization (WHO) report, [3] there is a high unmet need for antenatal care visits, skilled birth attendance, DTP containing vaccines, antiretroviral therapy for HIV, treatment of Tuberculosis as well as adequate access to clean water and sanitation. Furthermore, in India, diseases such as diabetes and impaired glucose tolerance show a positive association with age, history of diabetes, and other such factors.

Moreover, the age standardization of diabetes was 12.1%, and standardization of impaired glucose tolerance was 14.0%, with no difference in genders as of 2001 [2].

Things based WBANs provide us with facilities to monitor insulin levels of patients remotely. Thus, notifying patients and doctors if the level falls above or below a certain threshold with the help of IoT. WBANs are a form of Wireless Personal Area Network that utilizes Radio Frequency (RF) to network a series of wearable computing devices with a sensor or actuator capability. These sensors work within a close vicinity (surface-mounted), implanted, or embedded under the skin [4]. According to the IEEE 802.15.6-2012 standard, Body Area Networks (BANs) also require "Quality of service (QoS), extremely low power, and data rates up to 10 Mbps to be supported while simultaneously complying with strict non-interference guidelines where needed" [5] WBANs may empower universal health services and could prompt proactive, and even remote, indicative of ailments at early stages [7]. The thing based WBAN can be realized using an array of sensors and a gateway. A gateway allows protocol conversion in case the set of sensors being used are homogeneous in nature. This facilitates compatibility amongst nodes. The gateway can either be a computer system or even a mobile device such as a smartphone. The device is capable of receiving sensory data from various nodes and then via an appropriate medium such as Wi-Fi or Zigbee. The data can either then be logged locally and transmitted in batches or sent in real-time. However, the network must notify emergency services immediately in case of an emergency (i.e., sensors exceed a threshold value for a prolonged time slice). This data is typically stored on a Remote health monitoring (RHM) server and can be further used for analysis. Figure 1 shows the architecture of Secured smart WBAN health monitoring system. IoT connects Physician, Emergency care, Medical Server, and Care Giver through smart devices. A primary characteristic of WBANs is continuous monitoring and supervised recovery as a part of the diagnostic procedure. Another important characteristic to note is the lack of wires. Wires tend to cause discomfort and restrict the patient's movements. The Gateway or a personal server connects to a network of sensors, servers, and other services. Traditionally, this data was collected offline and support for large data collection, while knowledge discovery was almost non-existent. The gateway utilizes Zigbee, GPRS, and Bluetooth/WLAN, providing the user with a wide range of connectivity.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author

Jacob John*, School of Computing Science and Engineering, Vellore Institute of Technology, Vellore, India

Mariam Sunil Varkey, School of Computing Science and Engineering, Vellore Institute of Technology, Vellore, India

Selvi M, School of Computing Science and Engineering, Vellore Institute of Technology, Vellore, India

Retrieval Number: A4242119119/2019©BEIESP
DOI: 10.35940/ijitee.A4242.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Furthermore, the patient can be seen using a motion sensor, blood pressure, and ECG monitor, which are standard apparatuses used for monitoring patients. The WBAN architecture can be further divided into three levels or stages:

A. The Sensor level or The Perception layer

The lowest layer of WBAN architecture is known as the sensor level. In traditional IoT architectures, this is also termed as the perception layer. This layer is responsible for obtaining raw and unprocessed data from the IoT sensor subsystem. It transforms information collected from the environment into a digital format. This information is typically collected from Wireless Sensor Networks (WSNs) or IoT sensors like ECG, humidity, temperature, blood pressure, etc. Communication technologies like Zigbee, Bluetooth, RFID, etc. handle how these devices transmit information to the server. WBAN networks tend to consist of devices or objects that have self-configuring capabilities and are based on standard and interoperable communication protocols. Some of these devices include Temperature Sensors, Electrocardiogram sensors (ECG), Electromyography sensors (EMB), Humidity sensors, Radiation sensors, Occupancy and Motion sensors.

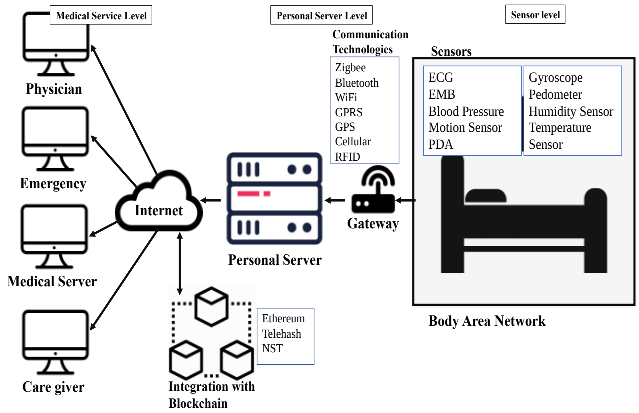


Fig. 1. Architecture of Secured smart WBAN health monitoring system

B. Personal Server Level

The personal server is the central processing unit of the system. It collects data from all the sensors by interfacing with them via a gateway. The personal server is used to process raw sensor information and store it in an appropriate medium such as secondary storage devices (hard drives, optical disks, solid-state drives), cloud services (Azure, Amazon Web Services, Google Drive) or on a blockchain network (Ethereum, NST, Telehash). It aggregates and processes the information gathered from sensors. The personal server also aids in providing a human interface to the system via a medical service level. The server also automatically regulates managed systems in response to sensor inputs. WBAN nodes are initialized, configured, and synchronized by this level. It also serves as a middleware layer that controls and monitors the operations of WBAN nodes. Furthermore, it continuously monitors all sensors and alerts the medical service level when there is an “alarm”.

C. Medical Service Level

Medical Service level consists of patients, doctors, nurses, or any stakeholder responsible for maintaining the health of the patient. The layer is used to observe the activity of the patient as well as issue altered guidance based on the new sensory input. It presents a comprehensive view of the entire managed system to the medical professionals. Furthermore, it provides a more detailed view in response to user requests. This layer is responsible for viewing and maintaining report logs and summarizing historical trends. In case the received data are out of range (from normal) or show a looming medical condition, then medical personnel is responsible for performing emergency services.

D. Blockchain

Blockchain has numerous features that have proved to be helpful to various industries. Blockchain can be defined as a distributed ledger that, with the help of consensus in the peer-to-peer network, forms a tamper-proof secure database of transactions [41]. In E-health, the majority of the application of the distributed ledger is for the management of health records.

II. SECURITY ATTACKS IN E-HEALTH

A. Security requirements in E-health

With the increasing demand for connectivity in IoT[50] devices within the domain of e-health, the number of devices in use is exploding. A global network of interconnected devices must be able to securely and efficiently handle these wireless connections. Short-range devices are categorized by their range of up to 100 meters and connectivity via unlicensed radio technologies like Wi-Fi, Bluetooth, and Zigbee. Every additional device makes the network open to more vulnerabilities. Another major challenge is the lack of standardization and the use of proprietary and closed source embedded softwares, technologies, and connection protocols. Some of the security requirements for WBAN networks namely integrity, privacy, confidentiality, availability, authenticity [46]-[48], [51],[52].

B. Unintended consequences of IoT in E-health

Security exposure in IoT devices could be as a result of unplanned security measures. With IoT, every device is connected to the Internet either directly, via a gateway, or through an access point. Some of the security risks include the lack of transport encryption, insufficient or poor authorization and authentication, inadequate software protection, poor privacy regulations, and insecure web interfaces. A breach in such devices could result in the leak of sensitive and personal information regarding names, physical address, e-mail, sexual preferences, date of birth, medical history, and health information. Compromised IoT devices can be used to coordinate a DDoS attack via a relay server, send spam, work as an entry point within a corporate or government network and serve as malware devices or trojan horses. Some of the unintended consequences in healthcare are hence as follows:

- Unforeseen spillovers or repercussions such as DoS attacks, network congestions, natural disasters, server downtime, and power blackouts. Loss of privacy of individuals due to data breaches.
- Data could get garbled during transmission or contract noise,

resulting in a loss of ability to maintain understanding and control of the original data.

- Exploitation of vulnerabilities causing amplification of the surface of attacks.
- Amplification of the digital divide either due to the lack of funding or as a result, social changes such as growing new professionals and assimilation of new skills.
- Lack of the ability to forecast, predict, and mitigate threats proactively and reactively as the primary focus is on patient care.

C. Security Risks and Challenges in E-health

The Open Web Application Security Project or OWASP has assembled a list of the top 10 security risks and privacy concerns for IoT [49]. OWASP is a worldwide not-for-profit organization whose primary focus is to improve software security. Table 1 summarizes a list of these security threats and provides a list of solutions for each individual threat. Furthermore, the list is ranked by the highest priority issues.

Table -I: Security risks and solutions in IoT

Rank	*Security Risk*	*Prevention Measures*
1.	Insufficient Authentication/ Authorization	Avoid weak default credentials Make sure password is complex and contains numeric, special, upper- and lower-case characters Secure against invalid privilege escalation
2.	Insecure network services	Protect against DoS, DDoS, and network fuzzing attacks by validating and alleviating congested network traffic Protect against buffer overflow and underflow vulnerabilities Ensure all ports are inaccessible or require authorization to access
3.	Insecure ecosystem and/or web interfaces	Fortify account enumeration Validate and harden session management Prevention against cross-site scripting (XSS) and SQL injection Lock users out of account upon unusual or insecure access
4.	Lack of any secure update mechanism	Provide sufficient security updates and patch bugs as early as possible; ensure that vulnerabilities and security flaws don't surface until after they've been patched The update server should be kept secure Every device should have the ability to update
5.	Use of outdated or insecure components	Provide sufficient security updates and patch bugs as early as possible; ensure that vulnerabilities and security flaws do not surface until after they've been patched Every device should have the ability to update Limit administrative capabilities on devices
6.	Insufficient protection of privacy	Avoid collection of unnecessary personal information Two-factor authentication, multi-factor authentication, biometric verification or security tokens must be implemented Disconnect storage devices and store sensitive data in hard copy form whenever possible
7.	Insecure data storage and transfer mechanisms	Ensure all data, irrespective of before transmission or stored device data is encrypted before transmission Ensure the transmission medium the data is sent using as well as remote communication mechanisms are encrypted Make sure only accepted encrypted standards are used and avoid the use of any proprietary encryption protocols Turn on auditing as well as directory auditing to track all changes Limit administrative capabilities on devices
8.	Lack of device management	Tightly control all resource access Maintain proper separation between administrative users and normal users Log all security events that take place on the devices and server
9.	Insecure default settings	Make sure all new devices are configured Ensure all devices are reconfigured after major updates or security patches
10.	Lack of physical hardening	Physical lockdown of servers and computers Remove any unnecessary storage media Prevent any external access via USB ports

III. METHODOLOGY

A. Works on Masquerade Attack

In such an attack, the attacker aims to masquerade himself/herself as an authorized user to gain higher privileges to access sensitive data. Masquerade attacks [6] are typically attempted by either bypassing security mechanisms or finding security gaps in the system using stolen login ids and passwords.

In Healthcare, the attack may be attempted from within the hospital itself by a medical faculty member or may originate from an outside client via some connection open to the hospital's local network. Masquerades may occur due to weak authentication mechanisms that make it easier for an attacker to obtain access to the system. Weak authentication can be defined as situations where the strength of the validation and verification mechanism for authorization is relatively weak compared to the assets being protected, which in this case is a patient's data. Once the attacker has enough privileges, he/she may modify or delete hospital records or even modify network configuration and routing information.

In WBANs, an attacker could compromise the security of a node. He/she can initiate a denial of service (DOS) attack to either the gateway or the RHM server itself, simply by masquerading a node. For example, during critical scenarios such as Intravenous (I.V.) therapy, an attacker could potentially deny access to the actuator that controls the I.V. drip-rate. This could lead to complications such as induced infiltration (when I.V. fluids leak into the surrounding tissues). Another scenario is when a "masquerade node captures the patient's physiological data" [8] and retransmits it to the RHM server at later durations. This could lead to mistreatment or overtreatment of a patient. This is because the server relies on real-time data logged from wireless sensors.

A proposed cost-effective and efficient solution for the prevention of such attacks could be the use of a “mutual authentication process before access network and data” [8] This middleware approach is software-based and can be implemented in WBANs provided a registration and verification phase exists between the user and network nodes. A 5-step process has been described in [8] that utilizes a pre-registration process to authenticate via the gateway for network accessibility. Upon successful authentication, the gateway performs a mutual authentication to check the validity of the RHM server. Once authenticated, it sends an acceptance message to the various other nodes. The session begins with a session key and a timer that determines the lifetime of the session.

B. Attacks on Wearables and Implantable Devices

Wearable devices are employed as an effective measure to monitor and diagnose a patient for a range of medical conditions. They serve as a step towards pervasive and ubiquitous computing due to their high uptime but lower power and bandwidth requirements. However, a significant security issue that persists is a direct attack on wearable or implantable sensors such as Medtronic’s Insertable Cardiac monitoring is another such example.

Monitor for patients experiencing arrhythmias. [9] A biodegradable cranial sensor for Intracranial Pressure (ICP) A Diabetes Therapy System (DTS) is a set of real-time remote healthcare monitoring devices that comprises primarily of an insulin delivery system and a glucose monitoring system. A DTS uses a wireless network for the transmission of data. An insult delivery system is comprised of a glucose meter, an insulin pump, and a remote control. [10] The insulin pump is directly tethered to the patient’s body for “autonomous administration of insulin through subcutaneous infusion” [4], while the remote regulates the insulin pump. Hence, security attacks on such devices could lead to severe consequences such as hyperglycemia or hypoglycemia.

According to [11], attacks such as eavesdropping, control of medical devices, and impersonation can quickly be conducted on a DTS “using public domain information and off-the-shelf hardware” through a wireless communication network. Wearable technologies (WT) are the latest technological invention with the introduction of Google Glass, Alexa Glasses, and various Smartwatches available in the market. WT are classified as computational and remote technology devices that can be worn directly attached to the body (such as on the wrist) or part of some clothing or accessory. However, they also present numerous amounts of security and privacy threats, as discussed in [25] by Ching and Singh. Some of these critical issues include poor authentication due to the simple gesture-based authentication scheme [44, 45] on Google glass.

A traditional cryptographic approach based on rolling code encoding and decoding can be used in a DTS, as suggested in [10]. Such systems have already been implemented and are being extensively utilized in automobile keyless entry systems. [12] Traditional remote-control systems send a fixed PIN to the device every time. The rolling code system, on the other hand, is an encoder embedded in the remote control as well as a decoder planted in the insulin pump.

The rolling code system works the following way:

1. The insulin pump and the remote control share an encryption key.
2. The key in the remote control can encrypt the sequence number and the control command.
   - The control command dictates the function of the insulin pump.
   - The sequence number increases by 1 for every communication packet.
3. The data is transmitted to the insulin pump.
4. To decode, the same key is used to decrypt the received data.
5. The decrypted received counter value is compared to the remote control’s sequence counter. If the difference between the two sequence numbers is within an acceptable range, the command is accepted. We can express the conditions as displayed in table 2.

The range is determined by the frequency of failed communication attempts. This is because the remote control’s sequence number is increased upon *every* communication packet sent. If the communication fails, the sequence numbers would then differ. Thus, allowing a ‘small window for errors.

Table -II: Rolling Code Conditions Algorithm

```
int range_lower, range_upper, sequence_counter,
        received_counter;
if $range\_lower \leq |received\_counter - sequence\_counter| \leq range\_upper$ then:
        valid AND accept;
        SYNCHRONIZE(recieved_counter,
                sequence_counter);
else:
        decline;
endif
```

The rolling code makes it almost impossible to launch a retransmission attack. [4] This is because the data sent is encrypted, and the sequence number needs to be consistent between the remote and insulation pump.

C. Denial of Service Attacks (DOS) in WBAN

When an attacker aims to render computer resources unreachable to its intended users, it is termed as a Denial of Service or DOS attack. In WBANs, an attacker could send a series of false data to either the RHM server or the gateway. Hence, it is necessary to protect the hub, where data is being collected from such attacks. This is to prevent it from intensively processing invalid data packets that, in the worst case, might get retransmitted to some of the other nodes. The attacker does this by masquerading a valid node. Hereby, receiving valid authentication information from the other notes. This, therefore, allows the attacker to send false packets that flood servers, sensors, and other such peripherals that receive data. Furthermore, in energy-constrained environments such as the WBANs, denial of service attacks can be expensive. DOS attacks could lead to a reduction in network uptime and a depletion of the battery power in sensors. According to [13], rejecting false data from masqueraded nodes should be an intrinsic and secure property built into sensors. However, cryptography is not enough to solve the problem of “persistent data injection attacks” (DOS attacks).

The proposed solution is a “distributed prediction-based secure and reliable (PSR) routing framework” for WBANs. This PSR routing framework would help effectively resist data injects while also increase routing reliability significantly within a WBAN network. A simulation “integrated with a hop-count based greedy routing procedure” showed that PSRs are 70% more successful at resisting data injections compared to a previous “static tree-based routing protocol”.

The incidental nodes to hop are provided by the underlying routing protocol in use. In PSRs, a node selects a link to forward the data sink based on the highest predicted link quality. Received signal power at the receiver’s end is used to characterize the quality of this mechanism. In addition to this, each node employs two authentication mechanisms to secure data communications – source authentication and destination authentication. For every received packet, a “lightweight hash-based data authentication” is performed. However, the nodes will disable source authentication if the neighbor set is not altering as per the predicted results. Source authentication necessitates “decryption operations which are more computationally demanding than data authentication” [13]. This is since established neighbors are already likely to be authenticated.

D. Key Abusers

Sometimes in the medical domain, users tend to share their access key with unauthorized users such as friends or family members. Attackers may employ social engineering mechanisms to extract keys from users to gain unauthorized privileges to the system. Furthermore, they could obtain access to a secret key used for the decryption of data. [4]

A proposed technique in [14], allows us to detect key IDs by examining the attacker’s device outputs for particular inputs. This enables us to trace back to the illegal key distributor. Every user is assigned a unique ID from a bit user identity space. Every user is designated as an attribute having two occurrences associated with it - one for bit value 1 while the other for 0. The primary objective is that during tracing operations, users with suspicious IDs are only able to decrypt a message. Thus, a pirate device by decrypting a tracing ciphertext, the ID of a device, is revealed. This is because a correct key has to be accessed, and the private device cannot differentiate between normal ciphertexts and normal operations.

E. Using Blockchain to improve resilience

Blockchain technology is resilient to various threats. This approach provides additional benefits of scalability, enhanced reliability, improved fault tolerance capability, etc. [36] The combined use of Blockchain and IoT can be extremely beneficial for many industries. IoT security can be improved by using identity and access management systems that are blockchain-based. Blockchain can also resolve challenges in IoT like cost constraints, cloud server downtime, susceptibility to manipulation. [41].

Linn and Koo [35] suggest a blockchain model for healthcare. A public blockchain is used as an access-control manager for health records whose storage is off-blockchain. The model aims at the blockchain being public and elements of scalability, access security, and data privacy. Scalability is ensured with the storage of medical data being in a data lake rather than on the blockchain itself. Data lakes, in addition to being highly scalable, can store various kinds of data in it. When it comes to access security and data privacy, a user has complete access and control over his/her own data. The access control permissions are not fixed, and policies are stored on a blockchain and are modifiable by the user.

Biswas et al. [36] used Blockchain to provide security for smart cities. The Smart City IoT framework consists of four layers: physical, communication, database, and interface. While no modifications were made to the physical and interface layer, blockchain was integrated into the communication layer, and the database layer consisted of distributed ledgers. The paper suggests the integration of protocols like Ethereum, NST, and Telehash to be added to the communication layer. A distributed ledger, either permissionless or permissioned, could be present in the database layer to store records. The use of private ledgers has been recommended for the benefit of efficiency and security.

Dorri et al. [45] recognize the need for reducing the significant energy, delay, and computational overhead induced with the use of a blockchain-based (BC) IoT system. Though BC systems provide decentralized privacy and security, they are unsuitable for resource-constrained environments. This paper suggests a framework that outlines the various core components of each tier of a smart home. One such important component is the “miner”. The home miner is in-charge of centrally processing incoming as well as outgoing transactions from the home’s Internet gateway. It is an always-on, high resource device that ensures privacy and security by preserving the BC and auditing and controlling communication. The framework was finally analyzed with respect to fundamental security goals. With the use of symmetric encryption and hashing, the framework is able to achieve confidentiality and integrity. Furthermore, availability is high due to the constraints of the number of transactions on the devices and miners. Finally, logging transactions and logged in the BC. Zhang et al.[38] propose how pervasive social network(PSN)-based healthcare can share data more securely with other nodes. Two protocols have been created. The first protocol is an enhanced version of the IEEE 802.15.6 display authenticated association, while the other has PSN nodes that utilize blockchain. The proposed system is divided into two parts of WBAN and PSN. The WBAN will use the first protocol to establish secure links while the PSN will utilize blockchain to share health data as per the second protocol.

Using the unique properties of blockchain, Azaria et al.[39] introduce MedRec, a decentralized record management system. Though this may not ensure complete security, it tackles some particular requirements like authentication, accountability, etc. Ethereum is used to create three different kinds of smart contracts. The smart contracts also help provide user notifications. The system node design includes Ethereum client as one of its four software components. This will ensure that the node can join and participate in the Ethereum blockchain network. For mining, two models have been proposed. One model is based on Ethereum’s incentivizing model, while in the second one, mining is done by medical stakeholders, and they are rewarded. Rifi et al. [40] also propose the use of blockchain for securely accessing and managing eHealth data.

Blockchain helps preserve the privacy and confidentiality of critical Electronic Health Records (EHR) being exchanged among patients and authorized personnel. In order to ensure security and sensors' low computational power, an off-chain database is used. IPFS database is hence proposed as a part of the off-chain database architecture. Ethereum blockchain is used via go-Ethereum (Geth), the Ethereum client, while SolidityC language is made use of for Smart contracts programming. Furthermore, a frontend was created with the use of HTML, CSS, and Javascript. For a future study, parameters can be changed in this implementation, and different tools can also be used.

Bahga et al. [42] implemented blockchain in a platform for Industrial IoT. The blockchain will aid in improving the Cloud-based Manufacturing(CBM) platform. Blockchain has the capability of creating a decentralized, peer-to-peer network. In the system, IoT devices have an interface board and a single-board computer (SBC). Every IoT device has an account in the blockchain network along with a wallet on the SBC. Smart contracts can also be implemented in this proposed platform. There are numerous applications of its platform, such as smart diagnostics and machine maintenance in healthcare.

IV. RESULTS ANALYSIS

The IoT reference model dictates a set of communication protocols to be used at each individual layer. Figure 3 presents a communication reference model listing all the major IoT protocols used at each layer. Similar to the TCP/IP model, the IoT model follows a horizontal approach. Furthermore, this model is more reliable than the OSI model. In addition to this, both models share the same five communication layers – *application layer, transport layer, network layer, link layer, and physical layer*. However, the IoT model is developed to focus primarily on small devices such as sensors, actuators, etc. Furthermore, the TCP/IP suite and the IoT reference model is protocol-oriented rather than model-oriented. This means protocols are developed first and then the models for them. In addition to this, this scheme also realizes cellular connections and 6LoWPAN. The IoT communication model also supports protocols for technologies such as Machine to Machine (M2M), Supervisory Control and Data Acquisition (SCADA), Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), cloud computing and so forth.

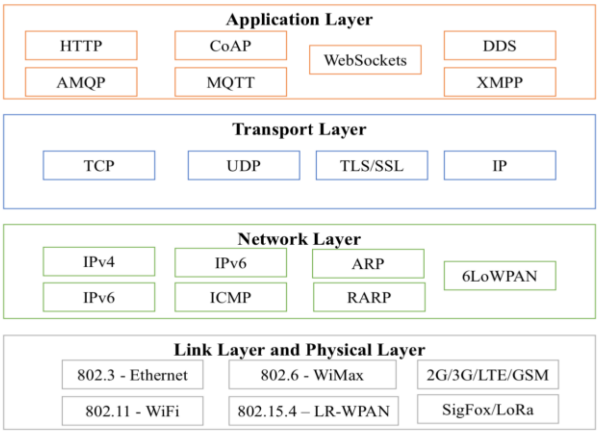


Fig. 3. An IoT communications reference model

The functionality of each communication layer along with the major IoT protocols is listed in table 3. A summary of all the attacks and defenses on SWBANs for layer-wise attacks can be found in Table 4.

A. *Physical Layer Attacks in WBANs*

Jamming and tampering are the two primary possible attacks in the physical layer. WBAN devices that are jammed or tampered with could thereby become safety-critical. Jamming disrupts wireless communication with the reduction of the signal-to-noise ratio at the receiver's end. A perpetrator deliberately uses interfering wireless signal to distort communication channels, sometimes, resulting in a denial of service attack [16]. This is because of the exposed nature of wireless mediums. Despite being typically used in an adversarial manner, jamming can be beneficial to those countering eavesdroppers on a network. A known jamming signal can be transmitted along with the medium by a trusted third party, which the receiver can decode using interference cancellation. The eavesdropper wouldn't be able to decode the transmission as he/she isn't aware of the jamming signal. Such cooperative or friendly jamming methods and rely on third parties to emit the jamming signal and receivers to decode it and present it in [17]-[19]. iJam [20], "a PHY- layer protocol for OFDM-based wireless systems", is another popular receiver side jamming protocol. Furthermore, work by [21] uses a variation of the above jamming method. The sender itself transmits the jamming signal combined with the data along the channel. The third party then sends out the interference signal to cancel out the jamming signal at the receiver's end but not for the attacker.

Wood et al. [22] propose JAM for mitigation and detection of jammed areas in a wireless sensor network. JAM uses a mapping approach that uses mainly existing data and allows nodes to collaboratively map out jammed regions in the network.

Table -III: WBAN Threats and solutions

Threats	*Solutions*
Masquerade attacks [6]	A Support Middleware Solution [8]
Attacks on Wearables and Implantable Devices [9, 45]	Cognition Based Adaptive WBAN Architecture [4], Defenses for a Diabetes Therapy System [10], Privacy Approaches Applicable to E-Health Systems [11], Keyless-Entry Systems [10], security and privacy vulnerability analysis [25], Improving Google glass security and privacy [44]
Denial of Service Attacks (DOS)	Exploiting Prediction to Enable Secure and Reliable Routing [13]
Key abusers [4]	Defending against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems [14], Novel key distribution [23]
Lack of resilience	Blockchain for health data [35], Securing smart cities using blockchain [36], Blockchain for IoT security and privacy [37], A secure system for pervasive social network-based healthcare [38], Blockchain-based solutions to security and privacy issues [39], Medrec [40], Can blockchain strengthen IoT [41] and Blockchain platform for IIoT [42]

Furthermore, this mapping service also provides feedback to routing and directory services that enable nodes to divert packets outside the uncongested area. Based on performance results, JAM can map regions in 1-5 seconds, which is adequate for a real-time response. Jain and Garg [23] propose a hybrid model of defense techniques against jamming attacks by combining three defense techniques – replication of base stations, evasion of the base station from a jammed location to an unjammed location, as well as multipath routing that looks for alternative unjammed paths for communication. Testing was done through simulation. It demonstrated the effects on the communication traffic throughput of the WSNs that the hybrid model had. These techniques recognize that Base Stations (BSs) are the most critical points of a WSN and the main focus for jamming attacks.

B. Link Layer Attacks in WBANs

Three link-layer attacks are collision, unfairness, and resource allocation attack. Collision is jamming in the link layer. In wireless sensor networks, if various sensors try to access the wireless channels at the same time, then nodes may suffer from a collision [27]. Unfairness refers to the situation when attacks hinder network performance instead of completely restricting access of legitimate nodes to the channel. In resource exhaustion attacks, repeated collisions and numerous retransmissions occur till the node dies [43].

In order to detect a collision, three statistical discrimination methods are introduced [27]. The IQ ADC output of the receiver implements these in practice. This determines periodically exchanges control packets among a base station node, a cluster head, and sensor nodes for the discovery of black hole attacks. Every sensor node also maintains a block hole table to avoid the selection of cluster heads as malicious nodes. The system is also evaluated using an NS whether the signal that is received is a valid collision-free packet or not. The proposed method provides the benefit of lesser computational complexity and shorter measurement period.

Unfairness is considered a weaker form of DoS. While this attack does not disallow access, it lowers the quality of service. Usage of small frames is a technique to help tackle unfairness. This means nodes will not have control of a channel for an extensive time period [15]. This, however, could lead to more framing overhead if the particular network typically sends long messages.

An authentication method [33] can help prevent exhaustion or resource allocation attacks. The primary purpose of any authentication mechanism is to confirm a client's identity before the commitment of resources to it by the server. This paper describes the use of stateless authentication protocol and client puzzles in preventing attacks.

C. Network Layer Attacks in WBANs

The homing attack is a network layer attack in which an attacker passively finds the location of a node and then uses active methods to attack the node. Misdirection and black holes are two other network layer attacks. In misdirection, messages are misguided in this path by the attacker so that it does not reach its intended destination [15]. Blackhole attack is when a compromised node helps the attacker to obtain access to other nodes within the network. This allows an opportunity to block packets instead of forwarding them during the reconfiguration of nodes [29]. NetSHIELD [28] tool can help in the prevention of network layer attacks. It consists of four modules with the goal to monitor incoming and outgoing packets, to match packets with stored rules, policies, and attack definitions that are present in the database, to block malicious packets, and alert the user when an attack has been detected. The modules are the UI module, a database module, a detection module, and a prevention module. As a solution to the misdirection attack, a SASO algorithm [30] is applied in the network context. The simulation was done of a Local Administrative Function using Omnet++. The results showed that it is capable of establishing secure link-layer communication. The algorithm was successful in maintaining a high rate of accurate data that was transferred. The energy consumed by attackers was also conserved. Kaur [29] implements a Black Hole Detection and Prevention (BHDP) algorithm to improve security and reliability in the defense section as well as civilian domains. BHDP uses a fuzzy logic algorithm to detect and prevent blackhole attacks in WSNs successfully. Furthermore, the efficiency and effectiveness of this technique can be improved with the deployment of numerous base stations to lessen the effect that black holes can have on data transmission.

D. Transport Layer Attacks in WBANs

Flooding attack in the transport layer occurs when an attacker sends numerous requests for new connections to the victim until either the maximum limit of the victim is attained, or resources have been exhausted [43]. Prevention of this attack can be done by restricting the number of connections. However, that would affect other processes at the victim and block future valid connections from taking place.

Aura et al. [33] identify an issue with regards to a client being unauthenticated and still consume the server's computation resources and memory. The clients induce the server to perform costly cryptographic computations by initiating a large number of protocols runs and flooding the server's resources. Aura et al. demonstrate the use of client puzzles of Juels and Barinard [26] coupled with stateless authentication protocols can be used to prevent flooding attacks on servers. Table 5 shows the layer-wise SWBAN attacks and defenses.

Table -V: Layer-wise SWBAN attacks and defenses

Layers	Attacks	Defenses
Physical layer	Jamming	iJam [20], Secret communication using artificial [21], JAM [22] and Hybrid model of defenses [23]
Link-layer	Resource allocation	Defense Strategy [31] and DOS-resistant authentication [33]
	Collision	Collision detection [27]
	Unfairness	Small frames [15]
Network Layer	Misdirection	NetSHIELD [28] and SASO algorithm [30]
	Black holes	NetSHIELD [28], Black Hole Detection and Prevention (BHDP) algorithm [29]
	Homing	NetSHIELD [28], Authorization [33], Monitoring, Ad Hoc Flooding Attack [32] and Redundancy
Transport Layer	Flooding	Stateless authentication protocols [26], Ad Hoc Flooding Attack [32], Client authentication [33] and DDoS attack methods [34]

V. CONCLUSION

There is much vulnerability associated with implementing ICTs in a Healthcare system. Attackers tend to exploit these vulnerabilities to capture sensitive data. These results in the privacy and legal violations in the healthcare industry, which could be damaging to the stakeholders involved in the attack. This paper surveys some of the attacks that could occur on S-WBANs – masquerade attack, attacks on wearables, DOS attacks, and key abusers. Furthermore, it also provides feasible and efficient solutions available to protect a user from such risks. In addition to this, this survey also mentions the utilization of new technologies such as blockchain to store medical data.

Although its transaction speed limitations, blockchain could serve as a decentralized network with high Byzantine fault tolerance for securely storing data. This paper also realizes the concern associated with falsifying sensor data and the endangering effect it could inflict. Attacks have been explored layer-wise with respect to IoT architecture along with various defenses against each of them.

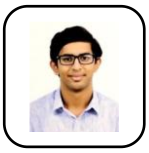
REFERENCES

1. Pavel Marceux, "Special report: the telecom consumer in 2020." *Euromonitor International Blog*. Euromonitor International, 27 Aug. 2013. Web. 29 Aug. 2018.
2. A. Ramachandran, C. Snehalatha, A. Kanpur, V. Vijay, V. Mohan, A. K. Das, et al. “High prevalence of diabetes and impaired glucose tolerance in India: national urban diabetes survey.” *Diabetologia*, vol. 44, no. 9, , pp. 1094–1101., 2001.
3. World Health Organization and World Bank. “Tracking universal health coverage, first global monitoring report”, 2015. Web. 29 Aug. 2018.
4. Dheeraj Rathee, Savita Rangi, S.K. Chakarvarti, V.R.Singh. “Recent trends in wireless body area network (WBAN) research and cognition based adaptive WBAN architecture for healthcare.” *Health and Technology*, vol. 4, no. 3, pp. 239–244, 2014.
5. Jonathan Goldberg. “IEEE 802.15.6-2012 - IEEE standard for local and metropolitan area networks - part 15.6: wireless body area networks.” *Standards.ieee.org*, IEEE, 6 Feb. 2012.
6. Sherali Zeadally, Jesus Tellez Isaac, Zubair Baig. “Security attacks and solutions in electronic health (E-health) Systems.” *Journal of Medical Systems*, vol. 40, no. 12, p. 263., 11 Oct. 2016.
7. Saeideh Sadat Javadi, M. A. Razzaque. “Security and privacy in wireless body area networks for health care applications.” Signals and Communication Technology *Wireless Networks and Security*, pp. 165–187, 2013.
8. Ndibanje Bruce, Mangal Sain, Hoonjae Lee. “A support middleware solution for e-healthcare system security.” *16th International Conference on Advanced Communication Technology*, pp. 44–47., 16 Feb. 2014
9. “Wearable & Implantable Technologies.” *Engineering in Medicine and Biology Society*, IEEE.
10. Chunxiao Li, Anand Raghunathan, Niraj K. Jha. “Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system.” 2011 *IEEE 13th International Conference on e-Health Networking, Applications and Services*, pp. 150–156, June 2011.
11. Ninad Desai, Hamid Shahnasser. “A light review of data security and privacy approaches applicable to e-health systems.” *Proceedings of the International Conference on Computing Technology and Information Management (ICCTIM)*, pp. 362–367, Apr. 2014.
12. Ansaf Ibrahem Alrabady, Syed Masud Mahmud. “Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs.” *IEEE Transactions on Vehicular Technology*, vol. 54, no. 1, pp. 41–50, 2005.
13. Xiaohui Liang, Xu Li, Qinghua Shen, Rongxing Lu, Xiaodong Lin, Weihua Zhuang et al. “Exploiting prediction to enable secure and reliable routing in wireless body area networks.” *2012 Proceedings IEEE INFOCOM*, pp. 388–396, 2012.
14. Shucheng Yu, Kui Ren, Wenjing Lou, Jin Li. “Defending against key abuse attacks in KP-ABE enabled broadcast systems.” *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Security and Privacy in Communication Networks*, pp. 311–329, 2009.
15. C. H. Hima Bindu, G. Surekha. “a novel approach for preventing jamming attacks in wireless sensor networks”. *International Journal of Computer Science and Technology*, *4*(4), 13–16, 2013.
16. Kanika Grover, Alvin Lim, Qing Yang, “Jamming and anti-jamming techniques in wireless networks: a survey.” *International Journal of Ad Hoc and Ubiquitous Computing*, *17*(4), 197-215, 2014.
17. Lifeng Lai, Yingbin Liang, H. Vincent Poor, H. “A unified framework for key agreement over wireless fading channels.” *IEEE Transactions on Information Forensics and Security*, *7*(2), 480-490, 2011.
18. Xiang He, Aylin Yener. “Secure communication with a byzantine relay.” *2009 IEEE International Symposium on Information Theory*, pp. 2096-2100. IEEE, June 2009.
19. Lun Dong, Zhu Han, Athina P. Petropulu, H. Vincent Poor. “Cooperative jamming for wireless physical layer security.” *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, pp. 417-420. IEEE, August 2009.
20. Dina Katabi, Shyamnath Gollakota. “iJam: jamming oneself for secure wireless communication.”, 2010.
21. R. Negi, S. Goel. “Secret communication using artificial noise.” *IEEE vehicular technology conference*, Vol. 62, No. 3, p. 1906, IEEE; 1999, September 2005.
22. A. D. Wood, J. A. Stankovic, S. H. Son. “JAM: A jammed-area mapping service for sensor networks.” *RTSS 2003. 24th IEEE Real-Time Systems Symposium, 2003*, pp. 286-297. IEEE, December 2003.
23. Sushil Kumar Jain, Kumkum Garg. “A hybrid model of defense techniques against base station jamming attack in wireless sensor networks.” *2009 First International Conference on Computational Intelligence, Communication Systems and Networks*, pp. 102-107. IEEE, July 2009.
24. Shu-Di Bao, Lian-Feng Shen, Yuan-Ting Zhang. “A novel key distribution of body area networks for telemedicine.” *IEEE International Workshop on Biomedical Circuits and Systems, 2004*, pp. 1-17. IEEE, December 2004.
25. Ke Wan Ching, Manmeet Mahinderjit Singh. “Wearable technology devices security and privacy vulnerability analysis.” *International Journal of Network Security & Its Applications*, *8*(3), 19-30. 2016.
26. Ari Juels, John Brainard. "Client puzzles: a cryptographic countermeasure against connection depletion attacks" Kent, S. (ed.). *Proceedings of NDSS '99 (Networks and Distributed Security Systems)*. pp. 151–165. 1999.
27. Fawaz Alassery, Waliz K. M. Ahmed, Mohsen Sarraf, Victor B. Lawrence. “Collision detection in wireless sensor networks through pseudo-coded ON-OFF pilot periods per packet: a novel low-complexity and low-power design technique.” *Computer and Information Science*, *8*(3), 13. 2005.
28. Prachi Korgaonkar, Ashish Patil, Nilesh Khochare. “NetSHIELD: countermeasure tool for network layer attacks.” *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, *1*, 91-94. 2012.
29. Jaspreet Kaur, Bhupinder Kaur. “BHDP using fuzzy logic algorithm for wireless sensor network under black hole attack.” *International Journal of Advance Research in Computer Science and Management Studies*, *2*(9), 142-151. 2014.
30. Maan Younis Abdullah, Gui Wei Hua, Naif Alsharabi, N. (2008, June). “Wireless sensor networks misdirection attacker challenges and solutions.” *2008 International Conference on Information and Automation*, pp. 369-373. IEEE, June 2008.
31. Djallel Eddine Boubiche, Azeddine Bilami, “A defense strategy against energy exhausting attacks in wireless sensor networks.” *Journal Of Emerging Technologies In Web Intelligence*, *5*(1). 2013.
32. Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong. “A new routing attack in mobile ad hoc networks.” *International Journal of Information Technology*, *11*(2), 83-94. 2005.
33. Tuomas Aura, Pekka Nikander, Jussipekka Leiwo. “DOS-resistant authentication with client puzzles.” *International workshop on security protocols*, pp. 170-177. Springer, Berlin, Heidelberg, April 2000.
34. R. K. C. Chang. “Defending against flooding-based distributed denial-of-service attacks: a tutorial.” *IEEE communications magazine*, *40*(10), 42-51. 2002.

35. Laure A. Linn, Martha B. Koo. “Blockchain for health data and its potential use in health it and health care related research.” *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, pp. 1-10. 2016.
36. Kamanashis Biswas, Vallipuram Muthukkumarasamy. “Securing smart cities using blockchain technology.” *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*, pp. 1392-1393. IEEE, December 2016.
37. Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram. “Blockchain for IoT security and privacy: The case study of a smart home.” *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pp. 618-623. IEEE, March 2017.
38. Jie Zhang, Nian Xue, Xin Huang. “A secure system for pervasive social network-based healthcare.” *Ieee Access*, *4*, 9239-9250. 2016.
39. Asaph Azaria, Ariel Ekblaw, Thiago Vieira, Andrew Lippman. “Medrec: Using blockchain for medical data access and permission management.” *2016 2nd International Conference on Open and Big Data (OBD)*, pp. 25-30. IEEE, August 2016.
40. Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher. “Towards using blockchain technology for eHealth data access management.” *2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME)*, pp. 1-4. IEEE, October 2017.
41. Nir Kshetri. “Can blockchain strengthen the internet of things?.” *IT professional*, *19*(4), 68-72. 2017.
42. Arshdeep Bahga, Vijay Madisetti. “Blockchain platform for industrial internet of things.” *Journal of Software Engineering and Applications*, 9(10), 533. 2016.
43. Alvaro Diaz, Pablo Sanchez. “Simulation of attacks for security in wireless sensor network.” *Sensors*, *16*(11), 1932. 2016.
44. Seyedmostafa Safavi, Zarina Shukur. “Improving Google glass security and privacy by changing the physical and software structure.” *Life Science Journal*, *11*(5), 109-117. 2014.
45. S. Geran. “Is Google glass a security risk?” (cited 19 Oct, 2015). 18 April 2014. [Online]
46. Engin Leloglu. “A review of security concerns in internet of things.” *Journal of Computer and Communications*, *5*(1), 121-136. 2016.
47. Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha. “Survey on secure communication protocols for the internet of things.” *Ad Hoc Networks*, *32*, 17-31. 2015.
48. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan. “Internet of things (IoT) security: current status, challenges and prospective measures.” *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336-341. IEEE, December 2015.
49. Pamela Rentz. “OWASP releases latest top 10 IoT vulnerabilities.”, 17 January 2019. Available: https://www.techwell.com/techwell-insights/2019/01/owasp-releases-latest-top-10-iot-vulnerabilities
50. K Thangaramya, K Kulothungan, R Logambigai, M Selvi, Sannasi Ganapathy, A Kannan, "Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT", Computer Networks, Elsevier, Vol. 151, pp.211-223, 2019.
51. M Selvi, K Thangaramya, Ganapathy Sannasi, K Kulothungan, H Khannah Nehemiah, A. Kannan, "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks", Wireless Personal Communications, Springer, pp.1–16, 2019.
52. Rakesh Rajendran, SVN Santhosh Kumar, Yogesh Palanichamy, and Kannan Arputharaj. "Detection of DoS attacks in cloud networks using intelligent rule based classification system." Cluster Computing, Vol.22, no. 1, pp. 423-434, 2019.

AUTHORS PROFILE

Jacob John is a student undergoing the Bachelor of Technology (B. Tech.) program in the School of Computer Science and Engineering (SCOPE) at Vellore Institute of Technology, Vellore, India. He is in his final year as of 2019. His main research interests are Data Science, Artificial Intelligence, and Machine Learning.



Mariam Sunil Varkey is a student undergoing the Bachelor of Technology (B. Tech.) program in the School of Computer Science and Engineering (SCOPE) at Vellore Institute of Technology, Vellore, India. She is in his final year as of 2019. Her main research interests are Information Security, Penetration Testing and Blockchain.

M.Selvi working as Assistant Professor (Sr.G) in School of Computer Science and Engineering, Vellore Institute of Technology, Vellore. She has completed her B.E in Electronics and Communication Engineering, M.E in Communication and Network Engineering from Anna University, Chennai and PhD program in the Department of Information Science and Technology College of Engineering Guindy Campus, Anna University, Chennai, India. She has published more than 15 papers in international journals and conferences. Her areas of interest are Wireless Sensor Networks and Data mining.

Table IV: Layers of the IoT reference model and their protocols

Layers	*Functions*	*Protocols*
Link layer: Corresponds to the physical and data link layer of the OSI and TCP/IP suite. Links connect adjacent nodes together and transfer datagrams from source to destination. Performs functions of the physical layer by transmitting as well as receiving raw bit streams over physical mediums.	*Link Layer functions* • Defines the format of packet exchange • Framing • Error detection • Transmission of datagrams • Flow and Error control • Random access • Encapsulation of bits as datagrams • Physical addressing *Physical Layer functions* • Bit synchronization • Transmission mode • Physical topologies • Bit rate control	IEEE 802.3 (i/j/ae/az) IEEE 802.15.4 IEEE 802.11(a/b/g/n/ac/ad) IEEE 802.16: 2G/3G/4G/5G
Network layer: Host to host transmission between networks. Also responsible for routing packets by managing traffic problems such as routing, switching, and congestion of data packets.	• Routing • Logical addressing • Internetworking • Fragmentation	IPv4 IPv6 6LoWPAN
Transport layer: Responsible for reliable end-to-end delivery of segments between application processes.	• End-to-end delivery • Reliable delivery • Addressing • Multiplexing • Flow and Congestion control • Segmentation and Reassembly • Service Point Addressing	TCP UDP
Application layer: Combination of the application, presentation, and session layer in the OSI model. Responsible for node-to-node communication and controls user-interface specifications	*Session Layer functions:* • Session establishment, maintenance, and termination • Synchronization • Dialog Controller *Presentation Layer functions:* • Translation • Encryption • Compression *Application Layer functions:* • Directory services • Mail services • FTAM-File transfer access and management • Network Virtual Terminal	HTTP CoAP WebSockets AMQP MQTT DDS XMPP